# Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform

Mohammed A. M. Abdullah*, S. S. Dlay and W. L. Woo
*Newcastle University, School of Electrical and Electronic Engineering, NE1 7RU, Newcastle Upon Tyne, U.K.*

Keywords: Biometric Protection, Biometric Watermarking, Discrete Cosine Transform, Iris Recognition, Template Security.

Abstract: With the expanded use of biometric systems, the security of biometric trait is becoming increasingly important. When biometric images are transmitted through insecure channels or stored as a raw data, they become subject to the risk of being stolen, faked and attacked. Hence, it is imperative that robust and reliable means of protection are implemented. Various methods of data protection are available and digital watermarking is one such techniques. This paper presents a new method for protecting the integrity of the iris images using a demographic text as a watermark. The watermark text is embedded in the middle band frequency region of the iris image by interchanging three middle band coefficients pairs of the Discrete Cosine Transform (DCT). Experimental results show that exchanging more than one pair will make middle band scheme more robust against malicious attack along with making it resistant to image manipulation such as compression. The results also illustrate that our watermarking algorithm does not introduce discernible decrease on iris image quality or biometric recognition performance.

## 1 INTRODUCTION

The growing need for security in recent years has resulted in the development of personal biometrics identification systems. Biometric is the science of establishing human identity using physical or behavior traits. The advantages of personal identification using biometric features are numerous, such as fraud prevention and secure access control (Vacca, 2007).

Although biometrics systems offer great benefits with respect to the traditional authentication techniques, the problem of ensuring the security and integrity of the biometric data is still critical. Hence, for a biometric system to work properly, the verifier system must guarantee that the biometric data came from a legitimate person at the time of enrollment (Yiwei et al., 2002). Encryption and watermarking can be used to achieve this purpose. However, encryption cannot provide security after the data is decrypted. On the contrary, watermarking involves hiding information into the host data for protecting its integrity, so it can provide security even after decryption.

A number of watermarking techniques are available for embedding information securely in an image. These can be broadly classified as transformation domain techniques (Yiwei et al., 2002; Deb et al., 2012; Wang et al., 2009; Sakib et al., 2011) and spatial domain techniques (Mukherjee et al., 2004; Singh et al., 2012). While the spatial domain techniques are having least complexity and high payload they cannot withstand low pass filtering and common image processing attacks (Dabas and Khanna, 2013).

Recently watermarking techniques have been used to protect biometric templates (Islam et al., 2008; Fouad et al., 2011; Isa and Aljareh, 2012; Majumder et al., 2013; Paunwala and Patnaik, 2014). In (Islam et al., 2008) the authors proposed a protection algorithm for the fingerprint image by watermarking it with a password extracted from the palm print of the same person. However, no experiments were performed by the authors to show the algorithm robustness against attacks. The authors in (Fouad et al., 2011) presented a scheme for protecting the iris template using a combination of cryptography and watermarking. The iris image is locked with a key and embedded in a cover image using combinations of Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT) as a watermarking algorithm. A second key is used to specify the embedding locations. Nevertheless, the two keys (iris key and embedding key) are required in iris extraction process. Later, (Isa and Aljareh, 2012) proposed a watermarking algorithm for protecting the biometric image. Face images were

*Mohammed A. M. Abdullah is also a staff member with University of Mosul and sponsored by the Ministry of Higher Education in Iraq to complete his PhD.


Abdullah M., Dlay S. and Woo W..
Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform.
DOI: 10.5220/0005305701080114
In *Proceedings of the 10th International Conference on Computer Vision Theory and Applications* (VISAPP-2015), pages 108-114
ISBN: 978-989-758-091-8

watermarked using the Cox watermarking algorithm (Cox et al., 1997). The face image acted as the username for identification while the watermark acted as a password for authentication. However, the problem with the Cox watermarking scheme is that the original image is needed at the watermark detector stage.

The authors in (Majumder et al., 2013) applied biometric watermarking by taking the DWT and the singular value decomposition of the host image to obtain an Eigen value vector. Next the iris features is extracted with DCT to obtain 200 coefficients and then embedded in the Eigen value vector derived from the host image. Despite of the good result reported by the authors, the drawback of this approach is that the feature extraction algorithm for iris cannot be changed. The work in (Paunwala and Patnaik, 2014) used the fingerprint and iris features as watermark for a cover image. The image is divided in blocks then each block is transformed into a two-dimensional DCT and classified as smoother block or edge block. The biometric features are embedded in the low frequency coefficients of the $8 \times 8$ DCT blocks while the edge block is eliminated.

Biometrics like fingerprint, face, and iris conveys unique biological information of a person. Nowadays, iris recognition is one of the most reliable biometric techniques that are extensively used for personal identification. To guarantee the reliability of iris recognition, a protection method is needed. The literature review revealed that a few research have been carried out so far to enhance the security of iris biometric through watermarking.

This paper presents a watermarking algorithm based on exchanging 3 middle band coefficients pair of the DCT using text data as watermarks for protecting the evidentiary integrity of iris images. The following section describes the Middle Band Coefficient Exchange (MBCE) algorithm. Section III explains the proposed algorithm. Experimental design and performance analysis are given in Section IV and Section V respectively. Finally, Section VI concludes this paper.

# 2 WATERMARKING ALGORITHM

Watermarking techniques in DCT domain allow an image to be divided into different frequency bands, so embedding the watermarking information in a specific frequency band becomes much easier (Langelaar et al., 2000). Current literature survey reveals that the middle frequency bands are most suitable for embedding the watermark because the low frequency band carries the most visual important parts of the image while the high frequency band is exposed to removal through compression and noise attacks on the image. Therefore, embedding the watermark in the middle frequency band does not affect the visual important parts of the image (low frequency) nor overexposing them to removal through attacks when high frequency components are targeted (Langelaar et al., 2000).

## 2.1 Watermarking Algorithm

The idea of the classical Middle Band Coefficient Exchange (MBCE) scheme was presented by (Zhao and Koch, 1995). Later, (Hsu and Wu, 1996) applied the DCT to implement the middle band coefficients embedding. The algorithm encodes one-bit of a binary watermark object into one $8 \times 8$ sub-block of the host image by ensuring that the difference of two mid-band coefficients is positive in case of the encoded value is 1. Otherwise, the two mid-band coefficients are exchanged.

Accordingly, after the DCT is applied to the image, an $8 \times 8$ block dimension is taken. Each DCT block consists of three frequency bands as illustrated in Figure 1. $F_L$ stands for the low frequency components of the block, while $F_H$ denotes the higher frequency components. $F_M$ is the middle frequency band and is chosen for embedding watermark information. This avoids significant modifications to the cover image while providing additional resistance to lossy compression techniques which targets the high frequency components (Hernandez et al., 2000).

For the frequency band $FM$, two locations from the DCT block ($DCT_{(u1,v1)}$ and $DCT_{(u2,v2)}$) are chosen as the region for comparison. After the watermark text is converted to a binary image, each pixel value is checked. The coefficients are swapped if the relative size of each coefficient does not agree with the bit that is to be encoded. Thus, if the pixel value in the binary text is 1, the DCT coefficient are swapped such that $DCT_{(u1,v1)} > DCT_{(u2,v2)}$. On the other hand, in

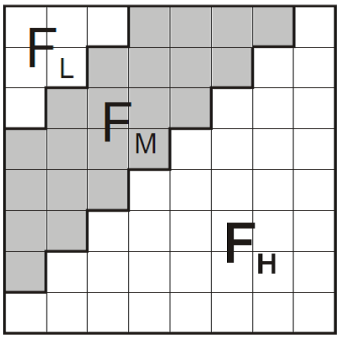


Figure 1: Frequency regions in $8 \times 8$ DCT block (Langelaar et al., 2000).

case of 0, they swapped so $DCT_{(u2,v2)} > DCT_{(u1,v1)}$. Hence, instead of inserting any data, this scheme is hiding watermark data by interpreting 0 or 1 with the relative values of the two fixed locations in $F_M$ region ($DCT_{(u1,v1)}$ and $DCT_{(u2,v2)}$). Swapping of such coefficients will not alter the watermarked image significantly, due to the fact that the DCT coefficients of middle frequencies have similar magnitudes (Zhao and Koch, 1995; Johnson and Katzenbeisser, 2000). In the extraction stage, the $8 \times 8$ DCT of the image is taken again, so it will decode a "1" if $DCT_{(u1,v1)} > DCT_{(u2,v2)}$; otherwise it will decode a "0" to form the watermark.

# 3 PROPOSED ALGORITHM

The previous scheme has a serious drawback. If only one pair of coefficient is used to hide the watermark data, it will become vulnerable to attack as the attacker can analyze some watermarked copies of an image to predict the location of these coefficients as well as destroy them.

To solve this problem, three coefficient pairs are chosen from the $F_M$ frequency band to increase redundancy and make the scheme robust against different attacks. The numbers of the pairs to be swapped in this paper were chosen as a trade-off between complexity and performance.

Moreover, to improve the robustness of the watermarking algorithm, we propose to add a watermark strength constant $k$ such that $DCT_{(u1,v1)} - DCT_{(u2,v2)} > k$. If coefficients do not meet these criteria, a constant value will be added to satisfy the relation.

## 3.1 Strength of Watermark

The strength of watermark has been increased by choosing an appropriate value of the proposed strength constant $k$. Increasing $k$ will degrade the image but it will reduce the chance of errors at the detection phase. Experimental results indicate that setting $k$ equals to 15 is the most suitable value in the perceptibility versus robustness. Therefore, the test has been conducted by keeping k=15.

## 3.2 Embedding Algorithm

Each $8 \times 8$ block of image will be used to hide one bit of watermark text. A binary text image ($W$) is taken as a watermarking object which can be interpreted as a 1D array of 1 and 0. The watermark text image carries the person bio-information such as name, ID and date of birth. The steps of the embedding algorithm are shown in Algorithm 1 while the flow chart is depicted in Figure 2.

**Algorithm 1:** Embedding algorithm.

**Input:** $X, W$
($X$: host image, $W$: watermarking text)
**Output:** $Y$
($Y$: watermarked image)

1: **loop**
2: $X_{8\times8(i)} = X$;
{subdivide the host image $(X)$ into blocks of $8 \times 8$ pixel}
3: $X_{DCT(i)} = 2D\text{-}DCT(X_{8\times8(i)})$
{Compute the 2D-DCT of each $8 \times 8$ block of the host image}
4: **for** $i = 1 \rightarrow size(W)$ **do**
5: **if** $W_{(i)} = 0$ **then**
6: exchange $DCT$ coefficients such that locations at $DCT(2,5), DCT(3,5)$ and $DCT(4,3)$ of the $8 \times 8$ sub-image will be larger than the locations $DCT(1,6), DCT(2,6)$ and $DCT(5,2)$ respectively
{Now adjust the three values such that their difference becomes larger than the constant $k$, thus: }
7: **if** $DCT(2,5) - DCT(1,6) < k$ **then**
8: $DCT(2,5) = DCT(2,5) + k/2$
9: $DCT(1,6) = DCT(1,6) - k/2$
10: **end if**
11: repeat step 7-10 for the other two coefficients: $DCT(3,5)$ and $DCT(4,3)$
12: **else if** $W_{(i)} = 1$ **then**
13: exchange $DCT$ coefficients such that locations at $DCT(2,5), DCT(3,5)$ and $DCT(4,3)$ of the $8 \times 8$ sub-image will be smaller than the locations $DCT(1,6), DCT(2,6)$ and $DCT(5,2)$ respectively
14: **end if**
{Now adjust the three values such that their difference becomes larger than the constant $k$, thus: }
15: **if** $DCT(1,6) - DCT(2,5) < k$ **then**
16: $DCT(1,6) = DCT(1,6) + k/2$
17: $DCT(1,5) = DCT(2,5) - k/2$
18: **end if**
19: repeat step 15-18 for the other two coefficients: $DCT(2,6)$ and $DCT(5,5)$
20: Take inversre DCT to reconstruct $Y$
21: **end for**
22: **end loop**

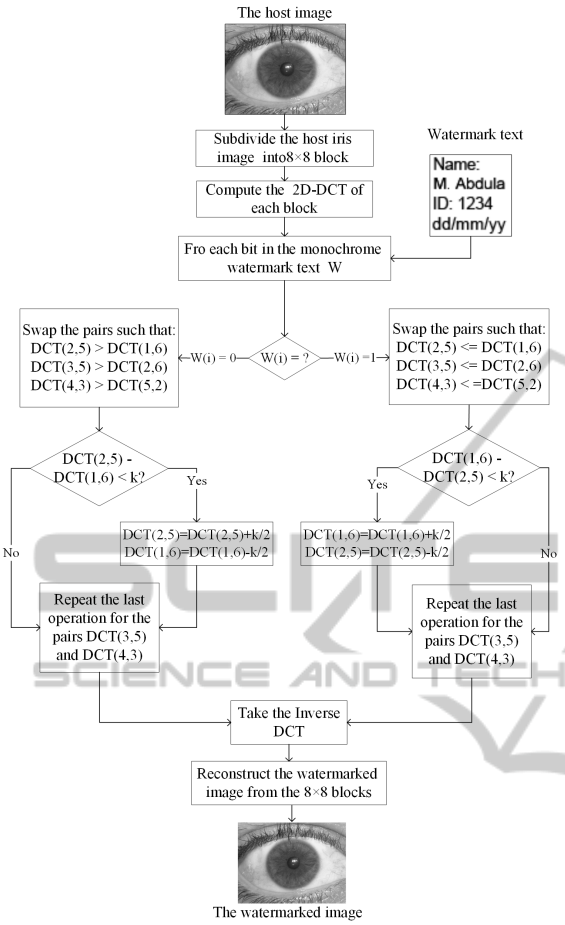


Figure 2: The flow chart of the embedding algorithm.

### 3.3 Detection Algorithm

Watermark extraction is the reverse procedure of watermark embedding. The steps of the detection algorithm are shown in Algorithm 2.

## 4 EXPERIMENTAL DESIGN

The proposed algorithm has been tested on session one of UBIRIS V1 iris database. The images were watermarked with $64 \times 64$ pixel text image shown in Figure 3(d) after converting it to a binary image.

## 5 RESULTS AND PERFORMANCE ANALYSIS

A robust watermarking algorithm should detect the embedded information reliably even if the watermarked image is degraded by different transformations. Besides robustness, a good watermarking algorithm should be imperceptible to the user as well as it should not affect the matching performance of the biometric system badly.

In order to evaluate our method, a set of different tests have been carried out on our proposed algorithm as shown in the next sub-sections.

**Algorithm 2:** Detection algorithm.

**Input:** $Y$
($Y$: watermarked image)
**Output:** $W$
($W$: binary text)
1: **loop**
2: $Y_{8\times8(i)} = Y$;
{subdivide the cover image $(Y)$ into blocks of $8 \times 8$ pixel}
3: $Y_{DCT(i)} = 2D\text{-}DCT(Y_{8\times8(i)})$
{Compute the 2D-DCT of each $8 \times 8$ block of the cover image}
4: **if** $DCT(2,5), DCT(3,5), DCT(4,3) > DCT(1,6), DCT(2,6), DCT(5,2)$ **then**
5: $W(i) = 1$
6: **else**
7: $W(i) = 0$
8: **end if**
9: **end loop**
10: reconstruct the binary text image $W$ from $W_{(i)}$

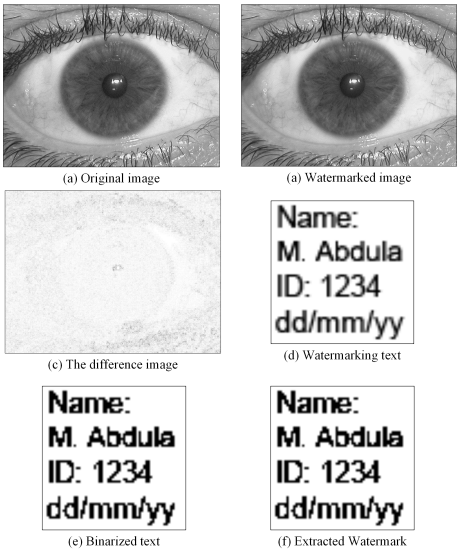


Figure 3: Perceptibility of the watermarked image; (a) Original image, (b) Watermarked image, (c) The difference image, (d) Original watermark, (e) binarized text and (f) the extracted watermark.

### 5.1 Watermark Perceptibility

The perceptibility is the similarity between the original and the watermarked image. Thus, the watermarked object should be imperceptible to the user. According to Figure 3(c) the difference between the original and the watermarked iris image is not noticeable to the naked eye without the help of image processing techniques.

To evaluate the performance of the watermarking algorithm, Peck Signal to Noise Ratio (PSNR) Bit Error Rate (BER) are calculated. The average PSNR between the original iris and the watermarked iris is 37.69 and the average BER is 0.257% while the average PSNR and BER of the extracted watermarking text are 84.25 and 0.0244% respectively.

### 5.2 Effect on Matching Performance

To find the effect of the watermarking on the iris recognition performance, Maseks approach (Masek, 2003) for iris recognition has been implemented and the Equal Error Rate (EER) is calculated for the non-watermarked iris images. After that, the proposed watermarking algorithm is applied to the same iris images and the EER is calculated again. Figure 4 illustrates the effect of watermarking of matching performance in term of Receiver Operating Characteristics (ROC) curve.

According to Figure 4, the proposed watermarking algorithm hardly affects the EER across all classes. Consequently, the recognition performance will not be affected by the proposed watermarking system.

### 5.3 Performance Against Compression and Noise

Apart from analyzing the change in perceptibility and matching performance, other considerations that may degrade the images were tested on our algorithm. There are several types of these degradations. For instance, the images are compressed when transmitting large image files over low bandwidth channel. In addition the iris images can be degraded if they are transmitted over a noisy communication channel.

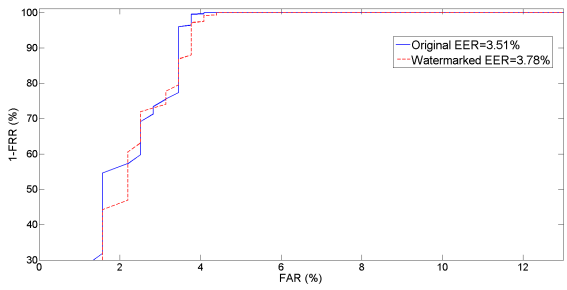


Figure 4: Effect of the proposed watermarking algorithm on iris recognition performance.

To simulate these effects, image compression algorithm, Joint Photograph Expert Group (JPEG) has been employed with different quality factors (Q). In term of the noisy channel, we applied the Additive White Gaussian Noise (AWGN) to the iris images with zero mean and variance equals to $10^{-3}$. Even with image compression and the added noise, the extracted text is still discernible. Figure 5 depicts the extracted watermarking texts from the manipulated iris images.

### 5.4 Performance Against Image Manipulations and Attacks

A robust watermarking algorithm should confront different signal processing signal processing distortions and attacks. A number of image manipulations were tested on our algorithm such as median filtering, histogram equalization and salt & pepper (noise density = 0.005). For each type of manipulation, the matching performances of the watermarked iris images are compared with the manipulated iris images in terms of ROC curves and EER. Moreover, the BER and PSNR of the extracted text are also calculated after these manipulations.

Figure 5 depicts the effect of different image manipulations on the extracted text while Figure 6 illustrates the effect of these image manipulations on iris

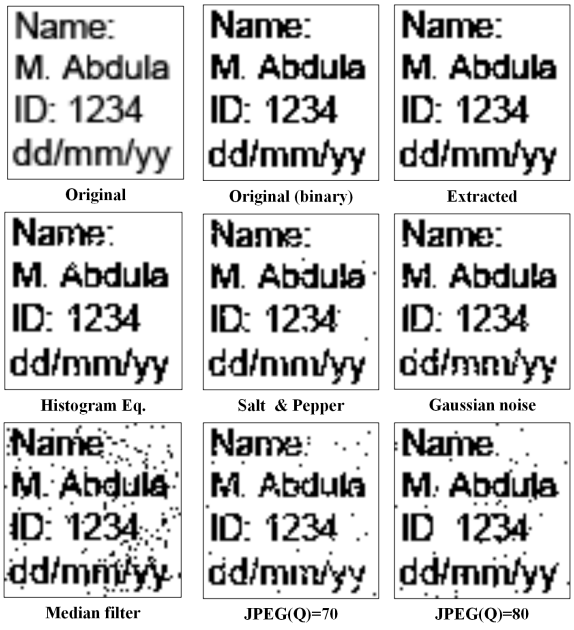


Figure 5: Extracted watermarked text after different attacks.

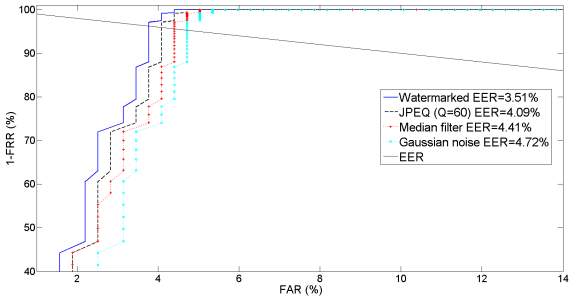


Figure 6: Effect of different manipulation on iris recognition performance using the proposed scheme.

recognition performance using the proposed method. According to Figure 6, no series loss in recognition performance is noticed in term of EER.

In order to appreciate the efficiency of the proposed method, the classical MBCE scheme (Hsu and Wu, 1996) is implemented and the proposed strength constant ($k = 15$) is introduced, then the same manipulations are applied to the watermarked iris images. Table 1 summarizes the PSNR and BER of extracted watermark text after JPEG, median filter, histogram equalization, Gaussian noise and salt & pepper noise using our method and the classical method.

The proposed algorithm sustained all above image manipulations and demonstrated that the watermarking scheme is resistant to different attacks.

Table 1: EER and PSNR of the extracted watermark after different manipulations using the clasical MBCE and the proposed algorithm.

| **Mnipulation type** | **Proposed Method** | | **Classical MBCE** | |
|---|---|---|---|---|
| | PSNR | BER | PSNR | BER |
| JPEG (Q=80) | 68.19 | 0.97% | 53.35 | 5.1% |
| JPEG (Q=70) | 60.13 | 2.3% | 44.35 | 8.23% |
| Median filter | 55.92 | 4.2% | 44.35 | 9.11% |
| Histogram equalization | 73.47 | 0.29% | 60.67 | 2.83% |
| Gaussian noise | 65.81 | 1.65% | 62.42 | 2.35% |
| Salt & pepper | 67.63 | 1.2% | 59.31 | 3.87% |

## 6 DISCUSSION AND CONCLUSIONS

This paper presents a novel scheme for image watermarking to protect the integrity of the biometric image. A binary text image which accommodates the bio data of the person to be authenticated is embedded in the iris image by interchanging the middle band coefficients using DCT. Exchanging more than one pair of the middle band coefficient make the watermarking scheme robust as it is impossible to the attacker to predict the three pairs that have been used to hide the data in each DCT block. Concurrently, the attacker cannot disturb all the middle coefficients as it will influence the image badly.

Experimental results indicate that the proposed algorithm is resistant to the common image manipulations such as JPEG compression, filtering and noising. The results also illustrate that our watermarking scheme does not significantly impede iris image quality or biometric matching performance. Empirical experiments show that swapping the pairs (2,5) and (1,6), (3,5) and (2,6), (4,3) and (5,2) in each $8 \times 8$ DCT block are visually imperceptible and maintain the iris recognition performance.

The proposed watermarking scheme is beneficial to the biometric system in a number of ways. For example, the biometric traits and the bio information of an individual are usually stored in independent databases. Digital watermarking integrates the biometric trait with the personal information in a single file and hence allows the data to be stored and extracted at the same time. Moreover, the integrity of the biometric trait can be verified from the extracted text.

One of the main advantages of our watermarking scheme is that it can be readily applied to any biometric image other than the iris image. On the other hand, the proposed algorithm does not require the original image for watermark extraction.

## REFERENCES

Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *Image Processing, IEEE Transactions on*, 6(12):1673–1687.

Dabas, P. and Khanna, K. (2013). A study on spatial and transform domain watermarking techniques. *International Journal of Computer Applications*, 71(14):38–41. study...no info.

Deb, K., Al-Seraj, M. S., Hoque, M. M., and Sarkar, M. I. H. (2012). Combined dwt-dct based digital image watermarking technique for copyright protection. In *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on*, pages 458–461.

Fouad, M., El Saddik, A., Jiying, Z., and Petriu, E. (2011). Combining cryptography and watermarking to secure revocable iris templates. In *Instrumentation and Measurement Technology Conference (I2MTC), 2011 IEEE*, pages 1–4. lock the iris with a key and embed it in a photo.

Hernandez, J. R., Amado, M., and Perez-Gonzalez, F. (2000). Dct-domain watermarking techniques for still images: detector performance analysis and a new structure. *Image Processing, IEEE Transactions on*, 9(1):55–68.

Hsu, C.-T. and Wu, J.-L. (1996). Hidden signatures in images. In *Image Processing, 1996. Proceedings., International Conference on*, volume 3, pages 223–226 vol.3.

Isa, M. R. M. and Aljareh, S. (2012). Biometric image protection based on discrete cosine transform watermarking technique. In *Engineering and Technology (ICET), 2012 International Conference on*, pages 1–5. Cox watermarking for face image.

Islam, M., Sayeed, M., and Samraj, A. (2008). Biometric template protection using watermarking with hidden password encryption. In *Information Technology, 2008. ITSim 2008. International Symposium on*, volume 1, pages 1–8.

Johnson, N. F. and Katzenbeisser, S. (2000). *A Survey of Steganographic Techniques*. Artech House Books. PN watermarking.

Langelaar, G. C., Setyawan, I., and Lagendijk, R. L. (2000). Watermarking digital image and video data. a state-of-the-art overview. *Signal Processing Magazine, IEEE*, 17(5):20–46.

Majumder, S., Devi, K. J., and Sarkar, S. K. (2013). Singular value decomposition and wavelet-based iris biometric watermarking. *Biometrics, IET*, 2(1):21–27. hiding iris image in Lena pic with key.

Masek, L. (2003). *Recognition of human iris patterns for biometric identification*. Thesis.

Mukherjee, D. P., Maitra, S., and Acton, S. T. (2004). Spatial domain digital watermarking of multimedia objects for buyer authentication. *Multimedia, IEEE Transactions on*, 6(1):1–15.

Paunwala, M. and Patnaik, S. (2014). Biometric template protection with dct-based watermarking. *Machine Vision and Applications*, 25(1):263–275.

Sakib, M. N., Alam, S. B., Sazzad, A. B. M. R., Shahnaz, C., and Fattah, S. A. (2011). A basic digital watermarking algorithm in discrete cosine transformation domain. In *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*, pages 419–421. a brief dicussion of watermarking method!

Singh, A. K., Sharma, N., Dave, M., and Mohan, A. (2012). A novel technique for digital image watermarking in spatial domain. In *Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on*, pages 497–501. LSB watermarking with no attacks.

Vacca, J. R. (2007). *Biometric Technologies and Verification Systems*. Butterworth-Heinemann.

Wang, W., Men, A., and Chen, X. (2009). Robust image watermarking scheme based on phase features in dft domain and generalized radon transformations. In *Image and Signal Processing, 2009. CISP '09. 2nd International Congress on*, pages 1–5. radon transfrom with DFT watermarking.

Yiwei, W., Doherty, J. F., and Van Dyck, R. E. (2002). A wavelet-based watermarking algorithm for ownership verification of digital images. *Image Processing, IEEE Transactions on*, 11(2):77–88.

Zhao, J. and Koch, E. (1995). Embedding robust labels into images for copyright protection. 211634 242-251.